As insurtech expands, password security gets left behind

By ID Federation

The beauty of insurtech is that hundreds of service providers offer innovative services that make insurance carriers more competitive. The not-so-beautiful flipside of insurtech is that carriers still require each of their business partners and users to maintain individual logins and passwords. The process works, but is redundant, inefficient and prone to security vulnerabilities. There is a way to streamline the workflow, reduce costs and increase both efficiency and security for every party in the insurance transaction.

To illustrate, here are before and after scenarios for carriers and their business partners.

Before the solution

1. **Many carriers set up proprietary rules requiring the changing of passwords and other measures aimed to create online security. Some business partners track and follow those various policies, however tedious and inefficient the process.**

2. But agency staff often resort to using a common office password, because keeping track of many passwords is confusing. Or they use one password for all the carriers with whom they conduct business, because maintaining individual passwords for each user for every carrier is inefficient. Or users make the job easier by writing down passwords on sticky notes or sharing password data files among themselves. In their frustration, they are creating risk daily.

3. When, inevitably, a user is locked out because of time lapses between logons or forgotten or expired passwords, the carrier must help. Carriers have indicated that nearly three-quarters of their help-desk calls are from users who forgot a password or need to reset one. Lost productivity costs up to $150 per incident.

After the industry solution

1. **With just one login on their agency management system, each user can access every participating carrier.**

2. The centralized identity management service is not only more secure, but quicker and easier than using individual passwords for every carrier.

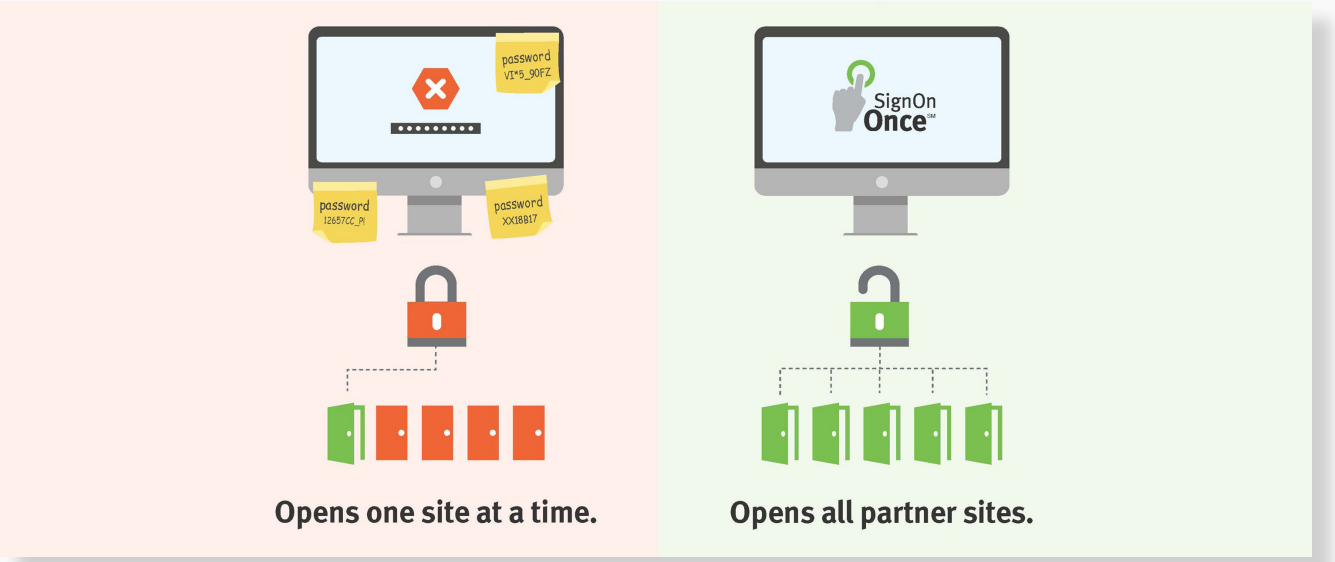
3. Agency owners can readily disable the credentials for any user just once for all participating carriers, rather than having to disable the user at each carrier separately.

4. Passwords can still be updated based on criteria established by the agency, but just one update will apply to all participating carriers. There's no more need to update passwords individually for each carrier.

SignOn Once by ID Federation (IDFederation.org) is the solution. It's not a product, but a concept. It's a trust framework that provides increased security, privacy and efficiency for all participants mutually in the insurance transaction. NU Property & Casualty ranks cybersecurity among the top five challenges now facing the insurance industry, and Deloitte observes that expense management in order to free up funds for digitalization is a leading concern for agencies. Such findings show that agencies need significant help with streamlining partnership workflows, including management of passwords for access to their carrier partners.

Success could be yours

Independent agency Foy Insurance Group and carrier partner MMG implemented SignOn Once by ID Federation on a pilot basis in 2019. The agency-carrier project proved that two firms could increase the security, effectiveness and efficiency of identity management. ID Federation is a nonprofit group of insurance industry leaders committed to working for the common good. It includes representatives from carriers, solution providers, industry associations and agencies. From an agency perspective, passwords cause slowness and inefficiency in a business that serves customers who demand speed and efficiency. SignOn Once will reduce costs for both for carriers and independent agencies.



WEBSITE

idfederation.org

OVERVIEW

ID Federation offers introductory information for insurance carriers and for solution providers. Your questions are welcome. Write info@idfederation.org.